

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of

David ARDITTI MODIANO, et al.

Conf.

Application No. **NEW NATIONAL PHASE**

Group

Filed December 14, 2005

Examiner

TRACEABLE METHOD AND SYSTEM FOR ENCRYPTING AND/OR DECRYPTING DATA,
 AND RECORDING MEDIA THEREFOR

INFORMATION DISCLOSURE STATEMENT
(SUBMISSION CONCURRENT WITH THE
FILING OF A NEW PATENT APPLICATION)

Assistant Commissioner for Patents
 P.O. Box 1450
 Alexandria, VA 22313-1450

December 14, 2005

Sir:

Pursuant to 37 C.F.R. §§ 1.97 and 1.98, and in fulfillment of the duty of disclosure under 37 C.F.R. § 1.56, applicant(s) hereby submit(s) an Information Disclosure Statement for consideration by the Examiner.

I. LIST OF PATENTS, PUBLICATIONS OR OTHER INFORMATION

The patents, publications, or other information submitted for consideration by the Office are listed on PTO-1449, attached hereto.

II. COPIES

- ☐ Copies of the U.S. patents or publications are not submitted since the USPTO has waived their submission for applications filed after June 30, 2003.
- ☒ Submitted herewith is a legible copy of (i) each foreign patent; (ii) each publication or that portion which caused it to be listed; and (iii) all other information or that portion which caused it to be listed.
- ☒ This application is a National Phase of a PCT application. Some or all of the documents listed on the PTO-1449 are not enclosed because they were cited in the International Search Report and copies should have been forwarded from the International Search Authority pursuant to the trilateral agreement between the USPTO, EPO and JPO, or they are U.S. patents or U.S. published applications. If copies are needed, please contact the undersigned.

III. CONCISE EXPLANATION OF THE RELEVANCE
(check at least one box)

AP20 Rec'd PTO 14 DEC 2005

a. ☒ **DOCUMENTS IN THE ENGLISH LANGUAGE**

The attached non U.S. patents, non U.S. patent application publications, foreign publications, or other information in the English language do not require a statement of relevancy.

b. ☐ **DOCUMENTS NOT IN THE ENGLISH LANGUAGE**

A concise explanation of the relevance of all patents, publications, or other information listed that is not in the English language is as follows:

c. ☒ **FOREIGN SEARCH REPORT OR ACTION**

An English language version of the search report or action that indicates the degree of relevance found by the foreign office is attached, thereby satisfying the requirement for a concise explanation. See MPEP 609(A)(3).

d. ☐ **OTHER**

The following additional information is provided for the Examiner's consideration.

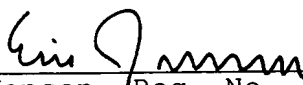
FEES

This Information Disclosure Statement is being filed concurrently with the filing of a new patent application; therefore, no fee is required.

If The Examiner has any questions concerning this IDS, he/she is requested to contact the undersigned.

Respectfully submitted,

YOUNG & THOMPSON


Eric Jensen, Reg. No. 37,855
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

EJ/lpp

Enclosures: ☒ Form PTO-1449(s)
☒ Documents
☒ Foreign Search Report
☐ Other: _____

10/25/05 60429
NEW NATIONAL PHASE

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (Use several sheets if necessary)	Attorney Docket No.: 0512-1307	Application No.: NEW NATIONAL PHASE
	Applicant: David ARDITTI MODIANO, et al.	
	Filing Date: December 14, 2005	Group Art Unit:

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing date (if appropriate)

FOREIGN PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation	
						Yes	No

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	BILLET O, GILBERT H: "A Traceable Block Cipher" ASIACRYPT 2003: 9 TH INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOLOGY AND INFORMATTON SECURITY (SPRINGER-VERLAG, HEIDELBERG, LECTURE NOTES IN COMPUTER SCIENCE 2894), November 2003 (2003-11), pages 331-346, XP002273113 ISBN: 3-540-20592-6 the whole document
	BONEH D; FRANKLIN M; "An efficient public key traitor tracing scheme" ADVANCES IN CRYPTOLOGY - CRYPTO'99. 19 TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, 19 August 1999 (1999-08-19), pages 338-353, XP002273114 Santa Barabara, CA, USA ISBN: 3-540-66347-9 page 338-page 343
	MATSUMOTO T; IMAI H: "PUBLIC QUADRATIC POLYNOMIAL-TUPLES FOR EFFICIENT SIGNATURE-VERIFICATION AND MESSAGE-ENCRYPTION" ADVANCES IN CRYPTOLOGY-EUROCRYPT '88. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, PROCEEDINGS. SPRINGER VERLAG, DE, 1988, pages 419-453, XP005688374 ISBN: 3-540-50251-3 cited in the application the whole document
	MENEZES; OORSCHOT; VANSTONE: "HANDBOOK OF APPLIED CRYPTOGRAPHY, PASSAGE" CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, 1997, pages 551-552, XP002273115 BOCA RATON, FL, USA ISBN: 0-8493-8523-7 page 551, paragraph 13.3.1-page 552
	PATARIN J; GOUBIN L; COURTOIS N: "Improved algorithms for isomorphisms of polynomials" ADVANCES IN CRYPTOLOGY-EUROCRYPT '98. APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, 4 June 1998 (1998-06-04), pages 184-200, XP002273116 Espoo, Finland ISBN: 3-540-64518-7 the whole document

EXAMINER:	DATE CONSIDERED
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.	

* English language abstract provided for the Examiner's convenience

EJ/lpp